Secure DoD Software

Considerations for the Vulnerability Market

Major Bradley C. Panton, Air Force Institute of Technology
John M. Colombi, Ph.D., Air Force Institute of Technology
Michael R. Grimaila, Ph.D., Air Force Institute of Technology
Robert F. Mills, Ph.D., Air Force Institute of Technology

Abstract. Every year, the DoD upgrades their information technology systems, allows new applications to connect to the network, and reconfigures the Enterprise to gain efficiencies. While these actions are to better support the warfighter and satisfy national security interests, they introduce new system vulnerabilities waiting to be exploited. This article recommends the DoD enter the vulnerability marketplace to mitigate the risk of a cyber attack using these undiscovered vulnerabilities. Through use of the vulnerability market, DoD will ensure information security is built into the application, minimize the number of distributed patches, and optimize investment in defense programs.

The vulnerability market, otherwise known as the market for "zero-day" vulnerabilities, has thrived ever since the first exploit was discovered on a computer system. Starting out as a black market forum where hackers could trade information for money, the vulnerability market is transitioning to a legitimate service. The vulnerability market now has growing influence over DoD software developers who regard computer security as a critical and required capability, and not just an added feature.

Historically in the DoD, as budgets contract, information systems aggregate. This phenomenon occurs primarily to offset the expense of maintaining a large workforce by automating much of the work accomplished by soldiers, sailors, airmen, and marines. As a consequence, an increase in the number of automated processes drives an increase in the number and complexity of information systems. The negative externality associated with this phenomenon is that as the number, complexity, and size of information systems increase, the prevalence of system flaws also increase. For example, a 2010 RAND study reported that a typical large code base can have a rate of one defect for every thousand software lines of code (KSLOC). Applying this defect rate to the Joint Strike Fighter's 18,000 KSLOC, there may be as many as 18,000 defects. While only a fraction of these defects would allow access to the IS and lead to unauthorized control of the system, an entirely defect-free information system is realistically impossible to achieve.

In order to mitigate the release of a system with undiscovered vulnerabilities, the DoD acquisitions process goes through great lengths to test the security of a product. Through developmental and operational test and evaluation, penetration testing, and the comprehensive information assurance certification and accreditation Process, the DoD seeks to identify and mitigate the risk of a possible cyber attacks resulting in the loss of money and life. These tests, coupled with the bolted on defense-in-depth strategy, have one critical shortfall; none of them analyze the system for undiscovered or obscure vulnerabilities.

The vulnerability disclosure lifecycle of a system typically consists of three common phases: learning, linear, and saturation [1], as shown in Figure 1. These phases are important as vulnerability discovery rates increase and decrease over time as the system passes through each window. The learning phase occurs immediately after the system is released to the public. During this phase, researchers and hackers become familiar with the system and gain better knowledge on how to break it. As a result of this lack of system knowledge, the vulnerability discovery rate during this phase tends to be low. Following the learning phase, the linear phase is characterized by a linear growth of vulnerabilities discovered by users. This explosion of discoveries is due to the system gaining market penetration and an increase in system familiarity. Once the system reaches obsolescence or as the number of undiscovered vulnerabilities diminishes, the vulnerability rate reduces as more users convert to a replacement and hackers lose interest. During this time the system is experiencing the saturation phase.

The length of time a system experiences each of the phases varies greatly. For example, if the hackers adapt to the new system quickly, the learning phase is short-lived. Furthermore, if the system is rife with vulnerabilities, the saturation phase may never be seen. Examples of these phases are readily seen in the commercial market. For demonstrative purposes, three popular systems are shown in Figure 2: Adobe Acrobat, the Java Development Kit (JDK), and Windows XP.

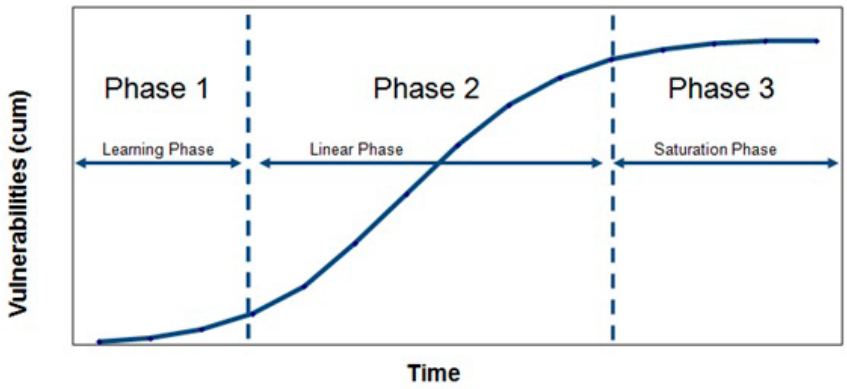

Figure 1: Vulnerability Disclosure Rate Phases [1]

As shown in Figure 2, there are clear delineations between the learning and linear phases. Also of note is the variability of phase lengths between software systems. Windows XP's learning phase was approximately three years where Adobe Acrobat experienced a 10-year learning phase. The causal factor of this variability is based on market share. For the Windows XP operating system, consumers quickly upgraded from the obsolete

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
DEC 2013		**00-00-2013 to 00-00-2013**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Secure DoD Software: Considerations for the Vulnerability Market	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **517 SMXS/MXDED,6022 Fir Ave,Hill AFB,UT,84056-5820**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Every year, the DoD upgrades their information technology systems allows new applications to connect to the network, and reconfigures the Enterprise to gain efficiencies. While these actions are to better support the warfighter and satisfy national security interests, they introduce new system vulnerabilities waiting to be exploited. This article recommends the DoD enter the vulnerability marketplace to mitigate the risk of a cyber attack using these undiscovered vulnerabilities. Through use of the vulnerability market, DoD will ensure information security is built into the application, minimize the number of distributed patches and optimize investment in defense programs.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**4**	

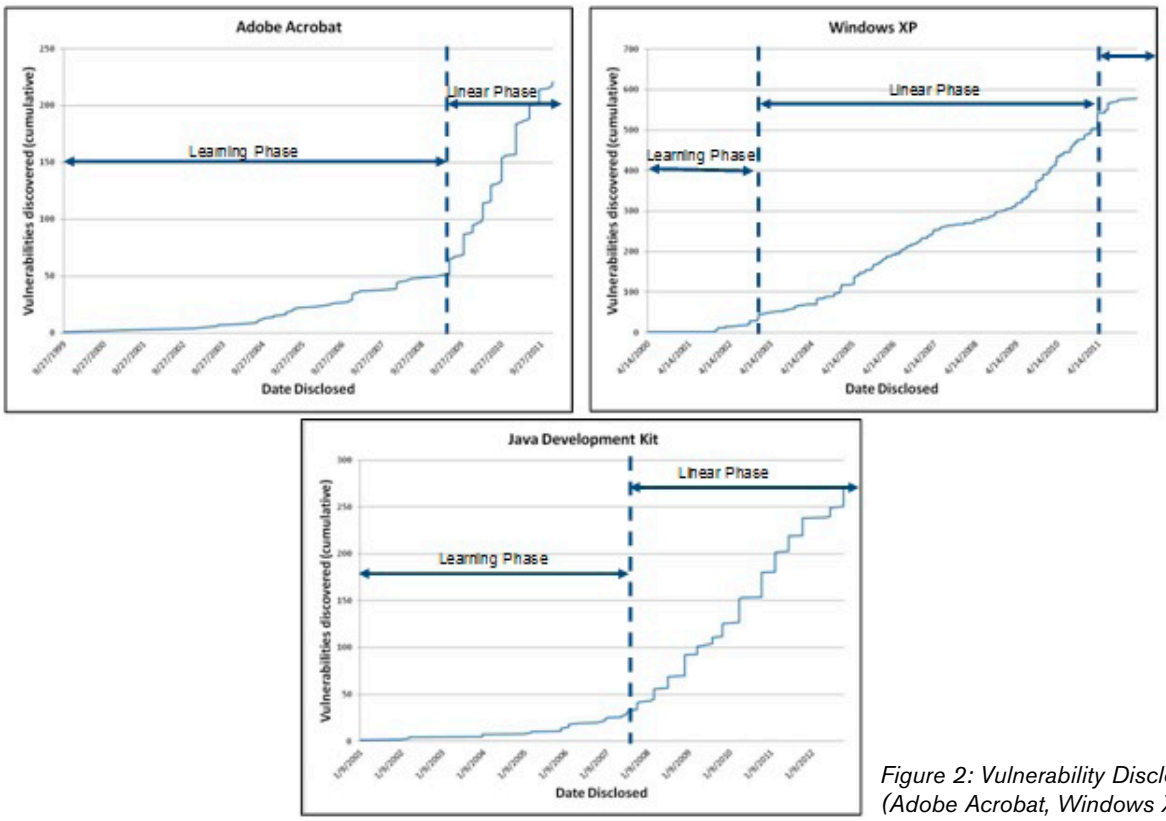

Figure 2: Vulnerability Disclosure Histories (Adobe Acrobat, Windows XP, JDK)

Windows 98/NT systems. The quick conversion ensured that Windows XP gained a large share of the market over a relatively short amount of time. In contrast, the Adobe Acrobat's share of the Portable Document Format market was limited by competitor saturation. It wasn't until July 2003 and the release of Adobe version 6.0 that the system gained popularity over similar proprietary systems. Shortly after the 2003 release, Adobe Acrobat entered the linear phase.

While the Common Vulnerabilities and Exposures database allows historical trend analysis, researchers have been searching for a model that will allow for predictive study. One such model is the Alhazmi-Malaiya Logistic (AML) model [1]. The AML model assumes that the shape of the vulnerability curve is restricted by market share and the number of the undiscovered vulnerabilities. The model proposes that the vulnerability discovery rate is given by the differential equation, Equation 1:

$$\frac{d\Omega}{dt} = A\Omega\,(B - \Omega)$$

Equation 1:

The two factors in Equation 1, AΩ and (B – Ω), relate to the application's market share and the number of system vulnerabilities. AΩ increases as market share increases and (B – Ω) decreases as the number of available vulnerabilities (B) decrease. Solving for Ω(t), the following logarithmic equation, Equation 2, is produced:

$$\Omega(t) = \frac{B}{BCe^{-ABt} + 1}$$

Equation 2:

In this equation, as time (t) approaches infinity, Ω(t) approaches B. Assuming the other variables remain constant, decreasing the number of vulnerabilities in a system (B) would flatten the shape of the s-curve. Stating that the market share (AΩ) remains constant is appropriate for DoD. More often than not, DoD acquires a specific application or system to meet a specified mission. Consequently, that system has a constant market share within the DoD. As a DoD system becomes obsolete and replaced, there is a resultant transition time; however, it has an accelerated pace which limits the saturation phase. As noted before, the delivery of a defect-free information system is impossible to achieve. The DoD can, however, attempt to deliver a system that is void of as many defects as possible, prior to deployment to the warfighter and operational use.

How does the DoD calculate the cost of a cyber attack? This question is not easily answered as there are many factors that determine total cost. In 2011, a global network security powerhouse, McAfee, reported the global economic impact to cyber attacks is as large as $1 trillion dollars. Furthermore, General Keith Alexander, commander of USCYBERCOM and Director of the NSA, estimated that the U.S. loses $250 billion annually to cybercriminals [2]. While a detailed account on how these estimates were formulated is not available, the public can assume the estimates were built using the following categories:

- Costs in anticipation of a cyber attack. Include the DoD's investment in the cyber security architecture (such as installing and implementing the Defense-in-Depth strategy).
- Costs as a consequence of a cyber attack. Takes into account the direct losses to an individual, service, defense industrial base, and overall national security.
- Indirect costs associated with a cyber attack. Includes damage to an organization's reputation, loss in national confidence, and time required to recover [3].

In the civilian sector, costs can be enumerated by the number of credit card numbers stolen, intellectual property theft, and pilfered insider trading information. In the defense sector, costs are measured as impacts to operations and intelligence activities. Based on the complexity of devising costs for cyber attacks, this article generalizes "cost" by calculating a probabilistic outcome using expected values.

In an effort to identify how the vulnerability market can strengthen overall system security, some basic formulas used to model the risk of a system to a particular vulnerability will be defined. For this analysis, we use the Single Loss Expectancy (SLE) formula to calculate the expected loss due to an exploited vulnerability. The SLE calculates a value based on the occurrence of a risk on a system. Calculating the SLE for a system incorporates two factors: the value of the at-risk asset (AV) and the asset's Exposure Factor (EF). The EF is a percentage of the asset's value that will be lost in the case of an attack. In the DoD, quantifying AV is difficult as it includes the value of information, value of lost productivity, the value of remediation, and (in extreme cases) the value of human life.

Suppose the DoD has an information technology asset (A) that is vulnerable to a particular system vulnerability (j). Let AV be the value of A and let EFj be the exposure factor for asset A when A is successfully attacked through the vulnerability j. Furthermore, let Pj be the probability of a successful attack on A through the vulnerability j. By incorporating these variables, the SLE for a successful attack results in Equation 3:

$$Single\ Loss\ Expectancy\ (SLE) = (AV \times EF_j) \times P_j$$

Equation 3:

The resultant SLE value is the cost risk that the organization incurs by not mitigating the probability of a particular vulnerability being exploited. Assuming an asset's value remains constant, the SLE can be reduced by either lowering the exposure factor or the probability of a successful attack.

It is unrealistic to believe a system in the DoD inventory is only susceptible to a single vulnerability. In fact, a DoD system may have hundreds of unknown vulnerabilities. To account for the entire set of vulnerabilities against a particular system, the Total Expected Loss for the set of all possible vulnerabilities {Tj} is the summation of SLEs. The sum of system SLEs, or Total Expected Loss (TEL), is expressed using Equation 4:

$$Total\ Expected\ Loss\ (TEL) = \sum_{j=1}^{n} SLE_j = \sum_{j=1}^{n} (AV \times EF_j) \times P_j$$

Equation 4:

For a given system, there are a total of n vulnerabilities. Now assume that the DoD engages in a strategy in which a set of vulnerabilities {Uj} are identified with set {Uj} being a subset of all possible {Tj}. By integrating this set of identified vulnerabilities, the new total expected loss (TEL') Equation 5 is:

$$TEL' = \left[\sum_{j \in T_j}^{n} (AV \times EF_j) \times P_j\right] - \left[\sum_{j \in U_j}^{n} (AV \times EF_j) \times P_j\right] - \sum_{j \in U_j}^{n} Price_j$$

Equation 5:

This set of identified vulnerabilities {Uj} effectively removes each corresponding SLE by changing the probability of attack from Pj to 0. Since {Uj} is a subset of {Tj}, the difference between the two summations is a positive value. As long as the cost of the purchased vulnerabilities (∑Pricej) is less than the difference, the expected net benefit is positive.

In acquiring secure software systems and applications, DoD could incentivize developers to use a mechanism that discovers the set of vulnerability disclosures {Uj} at a fair market price (∑Pricej) as part of development costs. One promising mechanism is the Vulnerability Market.

A vulnerability market is a setting where researchers are rewarded for discovered software vulnerabilities. On May 15th, 2013 the DHS announced that the government is entering the vulnerability marketplace by selling its stockpile of zero-day vulnerabilities to qualified vendors [4]. Furthermore, national media outlets have reported that the NSA actively researches and purchases zero-day exploits in order to gain access to an adversary's cyber assets [5]. While the precedence and legal framework are well established, the DoD has yet to realize the potential value of paying third party researchers for vulnerability information may have on DoD systems. Surprisingly, industry understands the issues of software vulnerability prevalence better than the DoD. In the past decade, dozens of vulnerability markets have sprung into existence based upon the perceived need to enlist non-organic researchers to report application vulnerabilities.

Today, the two primary players in the commercial vulnerability market are iDefense and Hewlett Packard TippingPoint's zero-day initiative. Between March 2003 and December 2007 an average 7.5% of the vulnerabilities affecting Microsoft and Apple were processed by either iDefense or TippingPoint [6]. Since 2007, the CanSecWest security conference has hosted the annual Pwn2Own bug challenge which rewards researchers for hacking into some of the most popular computer applications. During the 2013 Pwn2Own challenge, researchers were awarded $480,000 for cracking applications developed by Microsoft, Google, Adobe, Mozilla, and Oracle. Even more impressive, Google claimed theirs was the most secure operating system on the market by offering $110,000 for a browser or system level compromise delivered via a web page. At the end of the conference, the entire Google prize pot of $3.14M remained intact [7].

Each information system vulnerability has the probabilistic potential to cost the DoD resources. Although calculating the consequences of using a system with unknown vulnerabilities is difficult to quantify, it is certain that the discovery of a vulnerability prior to it being exploited by an adversary is more cost effective than remediating it post attack. Decreasing the probability and increasing the discovery rate of system vulnerabilities is the primary goal of using the vulnerability market for DoD systems. Not only will the discovery of an unknown vulnerability effectively reduce the probability of a successful attack, lifecycle operations, maintenance costs, and remediation efforts will also be reduced.

ABOUT THE AUTHORS

Major Bradley C. Panton is an acquisitions program manager for the United States Air Force. As a program manager, Major Panton has worked at the Electronic Systems Center, the Missile Defense Agency, and the National Geospatial-Intelligence Agency. He holds degrees in operations research, military operational arts and sciences, and cyber warfare.

E-mail: bradley.panton@us.af.mil

Dr. John M. Colombi is an Assistant Professor of Systems Engineering at the Air Force Institute of Technology. He teaches graduate courses and leads sponsored research in support of the Systems Engineering program. Dr. Colombi served at the NSA developing information security and managed communications networking research at the Air Force Research Laboratory.

E-mail: john.colombi@afit.edu

Dr. Michael R. Grimaila is an Associate Professor of Systems Engineering and Management and member of the Center for Cyberspace Research (CCR) at the Air Force Institute of Technology (AFIT), Wright-Patterson AFB, Ohio USA. He is a Certified Information Security Manager (CISM), a Certified Information Systems Security Professional (CISSP), a member of the ACM, a Senior Member of the IEEE, and a Fellow of the ISSA.

E-mail: michael.grimaila@afit.edu

Dr. Robert F. Mills is an Associate Professor of Electrical Engineering in the Department of Electrical and Computer Engineering, Air Force Institute of Technology. He teaches and conducts research in a variety of areas to include cyber security, network operations and management, electronic warfare, and systems engineering. He serves as the Curriculum Chair for AFIT's Cyber Warfare masters program and is a Senior Member of the IEEE.

E-mail: robert.mills@afit.edu

REFERENCES

1. Younis, A. A., Joh, H., & Malaiya, Y. K. (2011). Modeling Learningless Vulnerability Discovery using a Folded Distribution. The 2011 International Conference on Security and Management , 617-623.
2. Maass, P., & Rajagopalan, M. (2012, August 1). Does Cybercrime Really Cost $1 Trillion? Retrieved May 15, 2013, from Pro Publica: <http://www.propublica.org/article/does-cybercrime-really-cost-1-trillion>
3. Office of Cyber Security and Information Assurance. (2011, February). Retrieved May 17, 2013, from The cost of cyber crime: <http://www.cabinetoffice.gov.uk/resource-library/cost-of-cyber-crime>.
4. Schwartz, M. J. (2013, May 16). DHS Eyes Sharing Zero-Day Intelligence With Businesses. Retrieved May 17, 2013, from Information Week: <http://www.informationweek.com/security/vulnerabilities/dhs-eyes-sharing-zero-day-intelligence>.
5. Schneier, B. (2012, May 30). Forbes. Retrieved May 22, 2013, from The Vulnerabilities Market and the Future of Security: <http://www.forbes.com/sites/bruceschneier/2012/05/30/the-vulnerabilities-market-and-the-future-of-security/>.
6. Frei, S., Schatzmann, D., Pattner, B., & Trammel, B. (2009, June 25). Modeling the Security Ecosystem – The Dynamics of (In)Security. Retrieved May 22, 2013, from <http://www.techzoom.net/security-ecosystem>.
7. Thomson, I. (2013, March 8). Pwn2Own: IE10, Firefox, Chrome, Reader, Java hacks land $500k. Retrieved March 13, 2013, from <http://www.theregister.co.uk/2013/03/08/pwn2own_contest_cansecwest/>.